HAAGA-HELIA
ammattikorkeakoulu

Pääsyn- ja käyttövaltuushallinnan kehittäminen

Kari Peiponen

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2.12.2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

2.12.2014

Tietojenkäsittelyn koulutusohjelma

Tekijä tai tekijät Kari Peiponen	**Ryhmätunnus tai aloitusvuosi** 2011
Raportin nimi Pääsyn- ja käyttövaltuushallinnan kehittäminen	**Sivu- ja liitesivumäärä** 34
Opettajat tai ohjaajat Ahti Kare	

Tässä opinnäytetyössä tutkittiin tietojärjestelmien pääsyn- ja käyttövaltuushallinnan ongelmakenttää toimeksiantajan muuttuneessa toimintaympäristössä ja selvitettiin yleisesti alalla kehitettyjä ratkaisuja sekä menetelmiä.

Työn aikana toimeksiantajan nykytilanne selvitettiin ja analysoitiin sekä laadittiin kehittämissuunnitelma tilanteen parantamiseksi. Merkittävä osuus työstä liittyi toimintaprosessien selvittämisen ja prosesseissa esiintyvien ongelmakohtien analysointiin. Toimintaprosesseista laadittiin kuvaukset ja niihin liitettiin analyysin pohjalta tarpeellisiksi todetut parannukset.

Selvityksen ja analysoinnin perusteella laadittiin vaiheittain toteutettava identiteetin- ja pääsynhallinnan kehittämissuunnitelma. Kehittämissuunnitelman ensimmäisessä vaiheessa toteutettiin toimintaprosessien selvitys, analysointi ja tarvittavat muutokset. Uusien prosessien käyttöönottoon liittyi selainkäyttöinen käyttäjätietojen hallintatyökalu, joka toteutettiin opinnäytetyön yhteydessä. Kehittämissuunnitelman lopuksi laadittiin suositus toimenpiteistä, jotka perustuvat federoidun identiteetinhallinnan ja kertakirjautumisen teknologioiden hyödyntämiseen tulevaisuudessa.

Kehitetyn selainkäyttöisen sovelluksen avulla voitiin parantaa nykyisten identiteetinhallinnan prosesseja ja havainnollistaa keskitetyn identiteetin hallinnan hyötyjä käytännössä. Hallintatyökalulla voidaan muuttaa Active Directoryyn kytkettyjen käyttäjätunnusten attribuutteja hajautetusti LDAP-rajapinnan kautta käyttövaltuushallinnan prosessin eri vaiheissa.

Asiasanat
Pääsynvalvonta, identifiointi, sähköinen tunnistaminen, todentaminen, valtuutus, työprosessit.

HAAGA-HELIA
University of Applied Sciences

Abstract

2 December 2014

Degree Programme in Information Technology

Authors Kari Peiponen	**Group or year of entry** 2011
The title of thesis Improving corporate access control	**Number of report pages and attachment pages** 34
Advisor(s) Ahti Kare	

This thesis includes a study about corporate access control and identity management development in a changing information technology environment. Recently developed solutions and methods were studied and utilized to form a development plan for the client organization.

During this thesis the current situation of the organization was studied and analyzed. On the basis of the analysis, development suggestions were made to improve the current processes. As significant part of the work was focused on exploring current access control processes and analyzing the problem areas. The processes were analyzed and necessary improvements were implemented into the processes.

This thesis also includes a development plan, which is intended to be implemented in stages. The first stage of the development plan consisted of investigation, analysis and the implementation of process improvements. As a part of the process improvements, a web application was developed to maintain essential user information. At the end of the development plan several suggestions were introduced to develop federated identity management technology and other methods in the future.

A web application was developed in order to improve the current identity management processes and to demonstrate benefits of well-organized identity management. With the web application the organization can maintain user information and user attributes in Microsoft Active Directory along the different phases of access control processes. Maintenance of user attributes is done through LDAP-interface, which is included in the application.

Key words
Access control, identity management, identification, authentication, authorization, processes.

Sisällys

1 Johdanto

Tietojärjestelmien pääsyn- ja käyttövaltuushallinnan haasteet kasvavat nykypäivän organisaatioissa. Tietojärjestelmien ulkoistaminen ja hankkiminen palveluna (Software as a Service, SaaS) sekä pilvipalvelut (esim. Office 365) yleistyvät. Käytettävät ohjelmistot eivät enää välttämättä sijaitse omassa tietoverkossa, vaan niitä käytetään verkon kautta oman organisaation ulkopuolella sijaitsevista konesaleista. Identiteetin- ja pääsynhallinnan kehittämisellä voidaan saavuttaa tilanne, jossa samalla käyttäjätunnuksella ja salasanalla päästään kirjautumaan mahdollisimman moneen tietojärjestelmään. (Linden 2012, 8.)

Muuttunut toimintaympäristö asettaa haasteita organisaatioiden tietohallinnoille, koska tietojärjestelmiä ei enää voi helposti integroida perinteisesti käytössä olleisiin tietoteknisiin ratkaisuihin. Perinteiset ratkaisut on toteutettu liittämällä uusien tietojärjestelmien autentikointi organisaation omaan käyttäjätunnistuksen järjestelmään. Käyttäjätunnistuksen tietojärjestelmiä kutsutaan hakemistopalveluiksi. (Boyle & Panko 2014, 315.).

Pääsyn- ja käyttövaltuushallinnan käsitteet ovat laajentuneet sisältämään sähköisen identiteetin hallinnan. Sähköinen identiteetti on tietojärjestelmiin luotujen yksilöllisten tunnisteiden ja attribuuttien muodostama kokonaisuus, joka luodaan silloin, kun käyttäjälle tai tekniselle resurssille täytyy järjestää pääsy järjestelmään. Periaatteena tulisi olla se, että kuhunkin eri kohteeseen tulisi liittää vain tarvittava minimimäärä attribuutteja. (Boyle & Panko, 324.)

Sähköinen identiteetti voi sisältää varsinaisten tunnisteiden lisäksi muita attribuutteja, jotka kuvailevat identiteettiä. Esimerkiksi käyttäjätunnus, salasana ja sähköpostiosoite ovat identiteetin keskeisiä tunnisteita. Muita attribuutteja voivat olla puhelinnumero ja organisaation yksikkö sekä tehtävä organisaatiossa. Erilaisia attribuutteja voi olla lukuisa määrä ja ne voivat myös liittyä järjestelmään yhdistettäviin teknisiin ominaisuuksiin. (Linden 2009, 9-10.)

Ongelmaksi muodostuu se, että kuhunkin eri tietojärjestelmän voidaan luoda samalle henkilölle erillinen sähköinen identiteetti, jolloin ne viittaavat samaan henkilöön, mutta

ovat silti erillisiä asioita. Käytettävyyttä helpottavat tällöin kaikki ne tekniset menetelmät, jossa sama sähköinen identiteetti käy tunnisteena mahdollisimman moneen eri tietojärjestelmään. Identiteetteihin liittyviä lisätietoja eli attribuutteja hyödynnetään useissa eri toiminnoissa, joten myös näiden tietojen laatu ja eheys ovat merkittäviä asioita. (Linden 2012, 7.)

Teknisten ratkaisujen lisäksi merkittävä vaikutus identiteetin- ja pääsynhallinnan toteutuksessa on organisaation toimintaprosesseilla ja toimintatavoilla. Prosessit sitovat identiteetinhallinnan organisaation toimintaan (Linden 2012, 40.) Siten tiedon laadun sekä eheyden taso on aina lopulta riippuvainen ihmisten toiminnasta. Kyseessä on suuressa määrin johtamiseen ja prosessien toimivuuteen liittyvä ongelma, joka edellyttää sitä, että organisaatiossa on pystyttävä sopimaan tarvittavista määrämuotoisista toimintatavoista. (Linden 2012, 4).

Tässä opinnäytetyössä tutkittiin tietojärjestelmien pääsyn- ja käyttövaltuushallinnan ongelmakenttää muuttuneessa toimintaympäristössä ja selvitettiin yleisesti alalla kehitettyjä ratkaisuja sekä menetelmiä. Empiirisessä osassa selvitettiin toimeksiantajan pääsyn- ja käyttövaltuushallinnan arkkitehtuurin nykytilanne sekä laadittiin analyysin pohjalta tavoitetilan kuvaus. Kokonaistilanteen parantamiseksi laadittiin vaiheittain toteutettava kehittämissuunnitelma. Nykyiset käyttövaltuushallinnan prosessit kuvattiin ja tehtiin analyysin pohjalta prosessien parannusehdotukset. Uusien prosessien käyttöönottoon ja parantamiseen liittyi selainkäyttöinen käyttäjätietojen hallintatyökalu, joka toteutettiin opinnäytetyön yhteydessä.

1.1 Rajaus

Opinnäytetyön rajauksena ovat tietojärjestelmien pääsyn- ja käyttövaltuushallinnan prosessit ja menetelmät sekä työkalut toimeksiantajan nykyisessä infrastruktuurissa. Tarkasteltavaksi on rajattu kulunvalvonnan tietojärjestelmät, mobiilivaihteen tietojärjestelmä, talous- ja henkilöstöhallinnon tietojärjestelmät sekä omaan keskitettyyn käyttäjähakemistoon liitetyt tietojärjestelmät. Toimeksiantajan omaan Microsoft Active Directory hakemistopalveluun liitetyt tietojärjestelmät käsitellään yhtenä kokonaisuutena

ilman erittelyä, lukuun ottamatta Microsoft Office 365 pilvipalvelua, joka esitetään erillisenä kokonaisuutena.

Opinnäytetyön tuotoksena on vaiheittainen kehittämissuunnitelma. Ensimmäisessä vaiheessa käsiteltävä osuus työstä rajataan toimintaprosessien selvittämiseen ja prosesseissa esiintyvien ongelmakohtien analysointiin sekä uuden käyttäjätietojen hallintatyökalun rakentamiseen. Kehittämissuunnitelman toinen vaihe on rajattu tulevaisuuden tarpeiden arviointiin ja suosituksiin tehtävistä toimenpiteistä. Oman käyttäjähakemiston kehittämissuunnitelmat on rajattu koskemaan Microsoft Active Directory hakemistopalvelua ja Microsoftin tuotteisiin yhteensopivaa teknologiaa.

1.2 Keskeiset käsitteet

Active Directory	Tarkoittaa Microsoft Active Directory hakemistopalvelujen tuotetta, joka on kehitetty käyttäjätunnusten hallintaan. Tuotteesta käytetään yleisesti lyhennettä AD.
Attribuutti	Tarkoittaa tässä opinnäytetyössä tietojärjestelmien käyttäjätunnukseen tai sähköiseen identiteettiin liittyviä lisätietoja, kuten nimi, sähköpostiosoite, titteli, osasto tai yksikkö, jne.
Hakemistopalvelu	Tarkoittaa tietojärjestelmää, joka sisältää käyttäjätietojen tallentamiseen ja tietojen hakemiseen optimoidun käyttäjätietokannan eli käyttäjähakemiston. Palvelu sisältää tietoja myös teknisistä resursseista, kuten työasemista, palvelimista ja käyttöoikeusryhmistä.
IaM	(engl. Identity access Management, IaM) Tarkoittaa identiteetin- ja pääsynhallinnan kokonaisuutta.
Identiteetti	Tarkoittaa tässä opinnäytetyössä käyttäjän sähköistä identiteettiä, joka sisältää käyttäjätunnuksen ja siihen liittyvät lisätiedot (attribuutit).

Identiteetinhallinta	Tarkoittaa käyttäjän sähköisen identiteetin ja siihen liitettyjen käyttöoikeuksien hallintaa sekä näiden tietojen välittämistä eri järjestelmiin.
IdM-järjestelmä	(engl. Identity Management, IdM) Tarkoittaa sähköisen identiteetin eli käyttäjätunnusten ja tunnuksiin liittyvien attribuuttien (tietojen) teknistä hallintajärjestelmää.
Käyttäjähakemisto	Tarkoittaa hakemistopalvelussa sijaitsevaa käyttäjätietokantaa, joka sisältää käyttäjätunnuksen, salasanan ja muut attribuutit..
eDirectory	Tarkoittaa Novell eDirectory hakemistopalvelujen tuotetta, joka on kehitetty käyttäjätunnusten hallintaan. Tuotteesta käytetään yleisesti lyhennettä eDir.
Provisiointi	Tarkoittaa identiteetti- ja käyttövaltuustietojen välittämistä eri järjestelmiin. Tietojen välittäminen voidaan tehdä automaattisesti tai manuaalisesti.
SaaS	(engl. Software as a Service, SaaS*)* Tarkoittaa ohjelmistoa, joka on hankittu palveluna. Ostaja käyttää toimittajan ylläpitämää ohjelmistoa verkon välityksellä.

2 Pääsyn- ja käyttövaltuushallinnan perusteet

Tietojärjestelmiin pääsy tapahtuu tunnistautumalla, jonka jälkeen tunnistetulle sähköiselle identiteetille annetaan ennalta määritellyt käyttövaltuudet tietojärjestelmän resursseihin. Sisäänpääsystä ja käyttövaltuuksien perusteella suoritetuista toimenpiteistä täytyy jäädä raportoitavissa oleva jälki tietojärjestelmän lokeihin, siinä laajuudessa kuin organisaation toimintapolitiikka vaatii. Toimintapolitiikka on keskeinen pääsyn- ja käyttövaltuushallinnan toimintaprosessien määrittelyyn vaikuttava tekijä. (Boyle & Panko, 264.)

2.1 Sähköinen identiteetti käsitteenä

Sähköinen identiteetti koostuu attribuuteista, jotka jollakin tavalla kuvailevat kohteena olevaa henkilöä tai liittyvät henkilöön. Erityisen mielenkiintoisia ovat sellaiset attribuutit, jotka määritellyssä kontekstissa tai nimiavaruudessa yksilöivät tietyn henkilön. Tällaisia attribuutteja kutsutaan yksilöiviksi tunnisteiksi. (Linden 2009, 9.)

Sähköisen identiteetin käsite on muodostunut tietoverkkojen kehittymisen ja ohjelmistojen käytön laajentumisen myötä. Tietoverkon kautta käytettäviin ohjelmistoihin täytyy päästä kirjautumaan sisään ja todentamisen perusteella käyttäjät saavat ennalta määritellyt käyttövaltuudet tarvittaviin resursseihin. Sähköinen identiteetti on abstrakti käsite ja samalla henkilöllä voi olla lukuisia erilaisia sähköisiä identiteettejä käytössään (Linden 2012, 10.) Erilaiset identiteetit voivat olla myös muille käyttäjille anonyymeja, eli identiteetin omistavaa henkilöä ei välttämättä pysty tunnistaman identiteettiin liittyvän tunnisteen perusteella. (Linden 2012, 59).

Koska tietojärjestelmissä on periaatteena liittää identiteettiin vain minimimäärä attribuutteja, muodostuu eri järjestelmiin helposti saman henkilön osaidentiteettejä. Tämä tarkoittaa sitä, että yhdessä järjestelmässä on vain pieni osa henkilöön liittyvistä attribuuteista. Tällöin vasta useiden eri järjestelmien sisältämistä attribuuteista muodostuu yhdessä kokonaisempi kuva henkilön sähköisestä identiteettistä. Tämä onkin usein toivottu tilanne, koska henkilö ei välttämättä halua kenenkään pystyvan yhdistämään eri osaidentiteettejä. Tilanne muuttuu kuitenkin organisaatioiden toimintaan liittyvässä

kontekstissa. Toiminnan kannalta onkin toivottavaa pystyä yhdistämään eri tietojärjestelmissä olevia osaidentiteettejä ja liittämään ne samaan henkilöön, jolloin pääsyn- ja käyttövaltuushallinnan toimintoja on mahdollista parantaa. (Linden 2009, 10–12.)

2.2 Tunnistaminen eli autentikointi

Nykyisin henkilö voi luoda tietoverkoissa ja sosiaalisessa mediassa itse useita sähköisiä identiteettejä, mutta työntekijän roolissa työnantaja määrittelee henkilön sähköisen identiteetin ja siihen liittyvät tunnisteet sekä muut attribuutit. Sähköisen identiteetin todentaminen eli tunnistaminen on keskeinen toiminto tietojärjestelmien pääsynhallinnassa. Tunnistaminen tarkoittaa sitä, että identiteetille määritellyt yksilölliset tunnisteet voidaan käsitellä tietoteknisesti ja siten tunnistaa yksiselitteisesti kyseessä oleva käyttäjä tai tekninen resurssi. Käytännössä ongelmakenttä koskee pääasiassa henkilöihin liittyvää tunnistamista. (Linden 2012, 10.)

Tunnistamisen yhteydessä henkilön tulee esittää vaaditut tunnisteet, jotka voivat olla vain henkilön itsensä tietämiä tai henkilöön liittyviä asioita, kuten:

- Mitä henkilö tietää (salasana tai yksityinen avain/koodi),
- Mitä henkilöllä on (fyysinen avain tai älykortti),
- Mitä henkilö on (sormenjälki) tai
- Mitä henkilö tekee (salasanalauseen ääntäminen). (Boyle & Panko 2014, 264.)

Kaksi viimeistä menetelmää voidaan myös määritellä kuulumaan samaan, eli biometrisen tunnistamisen kategoriaan. Tunnistaminen perustui aikaisemmin merkittävässä määrin salasanoihin. Nykyään käytettävissä on kuitenkin laaja skaala erilaisia teknologioita, kuten toimikorttiin (smart card), toimiavaimeen (token), biometriseen tunnistamiseen ja kryptografiseen protokollaan liittyvät tekniikat. (Boyle & Panko 2014, 265.)

Vahvan tunnistamisen toimintoihin liittyvät biometrisen tunnistamisen menetelmät ja erityisesti kryptografiseen protokollaan perustuvat menetelmät. Kryptografinen protokolla perustuu vaikeisiin matemaattisiin sääntöihin ja se on siksi mahdollista vain kah-

den teknisen laitteen välillä. Esimerkiksi sirukortti tai fyysinen avain sisältävät kryptografisen protokollan toiminnot ja käyttäjä tietää salasanan, jolloin molemmat yhdessä muodostavat vahvan autentikoinnin suojattavaan kohteeseen. (Linden ym. 2011, 16.)

Suomessa vahvan tunnistamisen määrittelee laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617. Lain perusteella vahvaksi tunnistamiseksi hyväksytään sellaiset henkilön tunnistamiseen liittyvät menetelmät, jotka perustuvat yhtä aikaa vähintään kahteen alla mainituista vaihtoehdoista:

a) salasanaan tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltija tietää;
b) sirukorttiin tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltijalla on hallussaan; tai
c) sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan yksilöivään ominaisuuteen.

2.3 Käyttövaltuuksien määrittely eli auktorisointi

Sähköisen identiteetin todentamisen jälkeen täytyy tietojärjestelmässä antaa yksilöivän tunnisteen perusteella käyttöoikeudet tarvittaviin resursseihin. Käytännössä tunnistetulle käyttäjätunnukselle annetaan tarvittavat käyttöoikeudet ennalta määriteltyihin resursseihin. Käyttäjätunnus voi kuulua tekniselle resurssille (koneellinen käyttö ohjelmallisesti) tai reaalimaailman henkilölle. Käyttövaltuudet voivat olla tunnuskohtaisia tai roolikohtaisia. Yksittäisille tunnuksille voidaan määritellä oikeuksia suoraan eri resursseihin tai toimintoihin, mutta roolipohjaisen oikeusmäärittelyn tapauksessa tunnus liitetään ennalta määriteltyyn oikeusryhmään roolin perusteella. Tällöin on suurten tunnusmäärien tapauksessa helpompi hallita kokonaisuutta, kun tunnukset liitetään vain tarvittaviin käyttöoikeusryhmiin työroolin perusteella. (Boyle & Panko 2014, 266.)

Lindenin (2012, 30–33) mukaan pääsynvalvonnan menetelmät voidaan jakaa viiteen erilaiseen toimintamalliin, riippuen siitä miten hallinta halutaan toteuttaa:

1) Pääsynvalvontamatriisiin (Access control matrix) perustuvassa menetelmässä määritellään käyttäjäkohtaisesti eri käyttäjiin (rivit) liittyvät suojattavat kohteet (sarakkeet) ja niihin liittyvät oikeudet (solut). Käyttäjien ja pääsynvalvonnan kohteiden kasvaessa menetelmän hallinta käy työlääksi tai jopa mahdottomaksi
2) Rooliin perustuvassa menetelmässä (role-based access control, RBAC) käyttäjätunnuksille määritellään roolit joiden perusteella eri rooleille annetaan tarvittavia

oikeuksia suojattaviin kohteisiin. Yksittäinen käyttäjä voi kuulua useisiin eri rooleihin. Roolien ominaisuuksia ovat myös hierarkia ja periytyminen, jolloin eri rooleille voidaan määritellä alirooleja (lapsirooleja) ja niiden välille voidaan määritellä oikeuksien periytyminen.

3) Pääsynvalvonta voidaan toteuttaa myös attribuutteihin perustuvalla menetelmällä (attribute-based access control, ABAC), jolloin jonkin tietyn attribuutin perustella (esim. kotikunta ja syntymäaika) voidaan antaa tarvittavat oikeudet.
4) Pakotettu pääsynvalvontamalli (mandatory access control, MAC) on menetelmä, jossa käyttäjät jaetaan eri luokkiin ja vastaavasti suojattava tieto jaetaan eri luokkiin. Pääsynvalvonta perustuu kahteen yksinkertaiseen sääntöön. Ensimmäinen sääntö on, että käyttäjä ei voi lukea tietoa, jonka luokitus on hänen luokitustaan korkeampi. Toinen sääntö on, että käyttäjä ei voi kirjoittaa tietoa, joka saa matalamman luokituksen kuin käyttäjällä itsellään on. Reaalimaailmassa toimivan systeemin rakentaminen on osoittautunut vaikeaksi ja tiedonkulku eri luokkien välillä on kuitenkin toisinaan tarpeen.
5) Jäljitettävyyteen perustuva malli (accountability based access control) on enemmänkin toimintafilosofia. Mallin logiikka perustuu siihen, että varsinaiseen pääsynvalvontaan ei määritellä tiukkoja rajoja, vaan kaikki toiminta järjestelmässä tallennetaan lokeihin. Tällöin mahdollisten väärinkäytösten ja virheiden lähteet sekä toimenpiteet voidaan jäljittää lokitiedoista jälkikäteen. Käyttäjät ovat siis vastuussa teoistaan ja kaikki toimenpiteet saadaan tarvittaessa esiin.

Keskeisenä periaatteena käyttövaltuuksien määrittelyssä ja hallinnassa tulisi noudattaa vähimmän käyttövaltuuden periaatetta (principle of least permissions). Vähimmän käyttövaltuuden periaate tarkoittaa sitä, että kullekin työntekijälle tulisi antaa vain ja ainoastaan sellaiset käyttövaltuudet, jotka hän ehdottomasti tarvitsee työtehtäviensä suorittamiseen. Periaate tarkoittaa sitä, että käyttäjälle voidaan turvallisemmin lisätä oikeuksia jälkikäteen, kuin antaa varmuuden vuoksi liian paljon oikeuksia etukäteen. Liiallisten oikeuksien poistaminen jälkikäteen sisältää huomattavasti enemmän virhemahdollisuuksia ja riskejä verrattuna oikeuksien lisäämiseen myöhemmin. (Boyle & Panko 2014, 309.)

2.4 Jäljitettävyys ja raportointi

Tietojärjestelmien pääsyn- ja käyttövaltuuksien hallinnan voidaan sanoa perustuvan kolmen A:n menetelmään (AAA). Kirjaimet viittaavat sanoihin autentikointi, auktorisointi ja auditointi. Viimeiseksi mainittu käsite auditointi tarkoittaa sitä, että järjestelmien ylläpitäjien täytyy pystyä seuraamaan ja analysoimaan, mitä tietty käyttäjä tai käyttäjätunnus teki tietojärjestelmässä. Ongelmallista tai epäasiallista toimintaa tietojärjestelmien käytössä ei voida havaita ajoissa, mikäli järjestelmien käytöstä ei tehdä säännöllistä seurantaa. Oleellinen toiminto jäljitettävyyden ja raportoinnin toteuttamisessa ovat lokitiedostot. Lokitiedostoihin tulisi tallentaa kaikki oleelliset tapahtumat pääsyn- ja käyttövaltuushallinnan prosesseissa. (Boyle & Panko 2014, 310.)

Valtionhallinnon tietoturvaohjeistuksessa on määritelty virastoille tarkat ohjeet käyttövaltuushallinnan järjestelmien jäljitettävyys- ja raportointitoiminnoille. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt ohjeen (VAHTI 9/2006 2006, 26) mukaan hallintajärjestelmän tärkein periaate tulisi olla se, että kaikkien käyttövaltuuksiin liittyvien toimenpiteiden tulee olla jäljitettävissä ja raportoitavissa. Raportteja tulee olla mahdollista tuottaa ajantasaisesti ja niiden tulee sisältää tiedot käytössä olevista tunnuksista ja niihin liittyvistä attribuuteista sekä käyttövaltuuksista.

2.5 Toimintaprosesseja ohjaavat periaatteet

Tietojärjestelmien käyttövaltuuksia sivuava lainsäädäntö perustuu pääosin kahteen toimintaprosesseja ohjaavaan lakiin (VAHTI 9/2006 2006, 11). Julkishallintoa sääntelee hyvän tiedonhallinnan vaatimukset määrittelevä laki viranomaisten toiminnan julkisuudesta 21.5.1999/621 (eli julkisuuslaki) ja siihen kuuluvat säädökset, joita ovat asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030 sekä valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Kaikkia toimijoita sääntelee henkilötietojen käsittelyä määrittelevä sekä hyvän tietojenkäsittelytavan kehittämistä ja noudattamista edistävä henkilötietolaki 22.4.1999/523.

Julkisuuslaki määrittelee julkishallinnolle hyvän tiedonhallintatavan toteuttamisen puitteet. Hyvän tiedonhallintatavan määrittelyt vaikuttavat käyttövaltuuksien hallinnan pro-

sessien toteuttamiseen, koska tietoja käsitellään myös sähköisinä asiakirjoina tietojärjestelmissä. Julkisuuslain piiriin kuuluva valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa määrittelee selkeät vaatimukset käyttöoikeushallinnan ja käytön valvonnan toteuttamiseen valtionhallinnon virastoissa.

Henkilötietolain mukaan henkilötiedoilla tarkoitetaan kaikkia niitä tietoja, joilla yksittäinen henkilö pystytään tunnistamaan. Henkilötietojen käsittelyllä tarkoitetaan kaikkea tietojen tallentamista, käsittelyä, muuttamista ja luovutusta koskevia toimintoja. Laki velvoittaa jokaisen henkilötietoja käsittelevän laatimaan rekisteriselosteen kaikista niistä henkilörekistereistä, joissa henkilötietoja käsitellään.

Sähköiseen identiteettiin liittyviä tietoja käsittelevä tietojärjestelmä käsittelee selkeästi henkilötietoja, mutta silti niistä ei välttämättä tarvitse tehdä henkilötietolain edellyttämää rekisteriselostetta. Tämä johtuu loogisen rekisterin käsitteestä, joka tarkoittaa sitä, että käyttötarkoituksensa vuoksi yhteenkuuluvat henkilörekisterit voidaan katsoa kuuluvan samaan kokonaisuuteen. Tällöin organisaatiossa käyttäjätunnuksia käsittelevä tietojärjestelmä voidaan katsoa henkilökuntarekisterin loogiseksi alirekisteriksi, josta ei tarvitse laatia erillistä rekisteriselostetta. (Linden 2012, 63.)

3 Pääsyn- ja käyttövaltuushallinnan tasot

Pääsynhallinnan ensimmäinen toiminto on autentikointi, jonka jälkeen kirjautuneelle käyttäjälle tai tunnukselle annetaan ennalta määrätyt käyttövaltuudet tietojärjestelmiin. Käyttövaltuuksia tulisi myöntää vain sen verran, kuin henkilö tarvitsee työtehtäviensä suorittamiseen. Organisaatioiden sisällä työntekijöillä on käytössään useita eri palvelimia, joihin erillinen autentikointi olisi työlästä. Tämän vuoksi on kehitetty menetelmiä keskitetyn autentikointipalvelun toiminnoille. Toimintoja varten on kehitetty tuotteita, joita kutsutaan hakemistopalvelimiksi. Hakemistopalvelimet sisältävät myös käyttäjätietokantoja eli käyttäjähakemistoja. Identiteetinhallinta laajentaa prosessia ja mahdollistaa keskitetyn pääsynhallinnan toteuttamisen tietojärjestelmiin. Sovellusvuokrauksen yleistyessä on hajautetun tietoarkkitehtuurin tarpeisiin kehitetty federoidun identiteetinhallinnan menetelmiä pääsyn- ja käyttövaltuushallinnan toteuttamiseen. (Boyle & Panko 2014, 326.)

3.1 Organisaation sisäinen hallintataso

Yrityksissä ja julkishallinnon organisaatioissa tietoteknisiä resursseja käytetään omassa tietoverkossa kymmenillä, sadoilla tai jopa tuhansilla palvelimilla. Suojattavat resurssit ovat pääosin tiedostoja ja tietokantoja sekä ohjelmistoja, joiden kautta tietoja voidaan käsitellä. Tällöin autentikoinnin toteuttamiseen täytyy olla sellaisia teknisiä menetelmiä, joilla autentikointi voidaan suorittaa keskitetysti. Ratkaisuna ovat keskitetyt autentikointipalvelimet, joiden avulla käyttäjä pääsee useiden palvelimien resursseihin kirjauduttuaan ensin yhdelle palvelimelle. Autentikointipalvelimet käyttävät pääasiassa RADIUS tai Kerberos protokollia tiedonvälitykseen. Kerberos protokolla on pääasiallinen Microsoftin käyttämä autentikoinnin menetelmä Windows palvelimien arkkitehtuurissa. (Boyle & Panko 2014, 312–313.)

Kerberos protokolla on menetelmä, joka tarjoaa autentikoinnin toiminnot asiakkaan ja palvelimen välille symmetrisen kryptauksen avulla. Autentikointi keskitetään tarkoitukseen kehitetylle palvelimelle, joka suorittaa autentikoinnin. Palvelin antaa onnistuneen autentikoinnin jälkeen asiakkaan ja palvelimen välille suojatun tiketin, jota käytetään yh-

teyden muodostamiseen kaikkien saman autentikointipalvelimen piiriin kuuluvien palvelimien välille. Tiketin avulla asiakkaan ja palvelimen välille muodostetaan suojattu istuntoavain, jota käytetään hyväksytyn yhteyden muodostamiseen. Yhteys asiakkaan ja suojattujen palvelimien välillä on avattuna ilman uutta autentikointia niin kauan kuin istunto on voimassa tai yhteys katkaistaan. (Bertino & Takahashi 2011, 57.)

Keskitetyt autentikointipalvelimet eivät kuitenkaan riitä käytännön toiminnassa, vaan lisäksi täytyy olla käytössä korkeamman abstraktiotason sisältävä hakemistopalvelin. Hakemistopalvelin on tietokanta, johon voidaan tallentaa keskitetysti tiedot ihmisistä, verkkoon kytketyistä laitteista, ohjelmistoista ja tietokannoista. Hakemistopalvelin sisältää pääsyn- ja käyttövaltuushallinnan tarvitsemien tietojen lisäksi paljon muuta tietoa työntekijöistä sekä laitteista, jotka kytkeytyvät palveluun. (Boyle & Panko 2014, 315.)

Hakemistopalvelun yhteydessä puhutaan usein käyttäjähakemistosta, jolla tarkoitetaan hakemistopalvelun käyttäjätietoihin liittyvää osuutta. Yleisimmät organisaatioiden käytössä olevat hakemistopalvelujen tuotteet ovat Microsoft Active Directory, Novell eDirectory ja UNIX pohjainen Sun ONE (Boyle & Panko 2014, 320).

Hakemistopalvelujen yhteydessä merkittävä käsite on **luottosuhteet**. Luottosuhde tarkoittaa sitä, että toinen hakemistopalvelin voi hyväksyä tietoja toiselta hakemistopalvelimelta. Luottosuhteita voi olla kaksisuuntaisia tai yksisuuntaisia, riippuen siitä, mihin suuntaan tieto liikkuu hakemistojen välillä. Luottosuhde voi välittää tietoa molempiin suuntiin tai vain pelkästään toiseen suuntaan. Luottosuhteet voivat olla myös siirtyviä tai ei siirtyviä, riippuen siitä, onko luottosuhde määritelty siirtyväksi useamman hakemiston yli vai ei. Esimerkiksi, jos hakemisto A luottaa B hakemistoon ja C hakemisto B hakemistoon, niin A:n ja C:n välillä on luottosuhde vain jos luottosuhteiden siirtyvyys on voimassa oikeaan suuntaan myös hakemistojen B ja C välillä. Luottosuhteiden määrittelystä muodostuu kuitenkin helposti monimutkainen tehtävä ja virheet asetuksissa voivat johtaa tietoturvan heikentymiseen. On turvallisempaa määritellä liian vähän, kuin liian paljon voimassa olevia luottosuhteita. (Boyle & Panko 2014, 318–319.)

Hakemistopalvelujen yhteydessä merkittävänä standardina mainitaan usein myös LDAP-protokolla. LDAP (Lightweight Directory Access Protocol) on standardiin perustuva sisäänpääsyprotokolla hakemistopalvelun tietojen käsittelyyn. LDAP-protokollan juuret ovat X.500-hakemistopalvelussa, josta haluttiin kehittää kevyempi versio yleiseen käyttöön. Ensimmäinen LDAP-määritys tehtiin vuonna 1993 ja nykyisin on käytössä kolmas versio (RFC 2251). LDAP-hakemisto on eräänlainen tietokanta, joka optimoitu hakutoimintoihin. Hakemisto sisältää hierarkkisessa puurakenteessa avain-arvopareja, jotka sisältävät tietoa rakenteeseen tallennetuista merkinnöistä. Merkintä koostuu attribuuteista, jotka kuvaavat yksittäiseen olioon liittyvää tietoa, kuten esimerkiksi sähköpostiosoitetta. Attribuutit voidaan jakaa käyttäjäattribuutteihin ja toiminnallisiin attribuutteihin. Toiminnalliset attribuutit voivat sisältää tietoa hakemiston toiminnasta tai tilasta. (Linden ym. 2011, 2-3.)

Microsoftin kaupallinen Active Directory (AD) tuote perustuu LDAP-protokollaan, mutta sitä on laajennettu ja muunneltu huomattavasti. Tämän vuoksi se ei ole suoraan yhteensopiva standardin mukaisten määritysten kanssa. Käytettäessä Active Directoryn LDAP-rajapintaa, täytyy ottaa huomioon eroavaisuudet hakemiston rakenteessa ja attribuuttien nimeämiskäytännöissä. (Linden ym. 2011, 7.)

Merkittävää LDAP-määrittelyissä on, että se tarjoaa standardin mukaiset toiminnot hakemistopalvelussa olevien tietojen hakemiseen, lisäämiseen ja muokkaamiseen sekä poistamiseen. Autentikoinnin operaatioita ovat bind, unbind ja abandon. Bind muodostaa yhteyden palvelimeen, jos autentikointi on onnistunut, unbind sulkee yhteyden ja abandon keskeyttää toiminnon. Hakuoperaatioita ovat search ja compare. Search operaatiolla voidaan hakea tietoja hakemistorakenteesta ja compare operaatiolla voidaan testata, onko jollakin attribuutilla tietty arvo, jolloin vastauksena on true tai false. Päivitysoperaatiot, joiden avulla hakemistoa voidaan käsitellä, ovat add, delete, modify ja modify DN (rename), Päivitysoperaatiot tehdään kerralla loppuun asti, tai niitä ei suoriteta ollenkaan. (Linden ym. 2011, 4-5.)

3.2 Organisaatiorajat ylittävä hallintataso

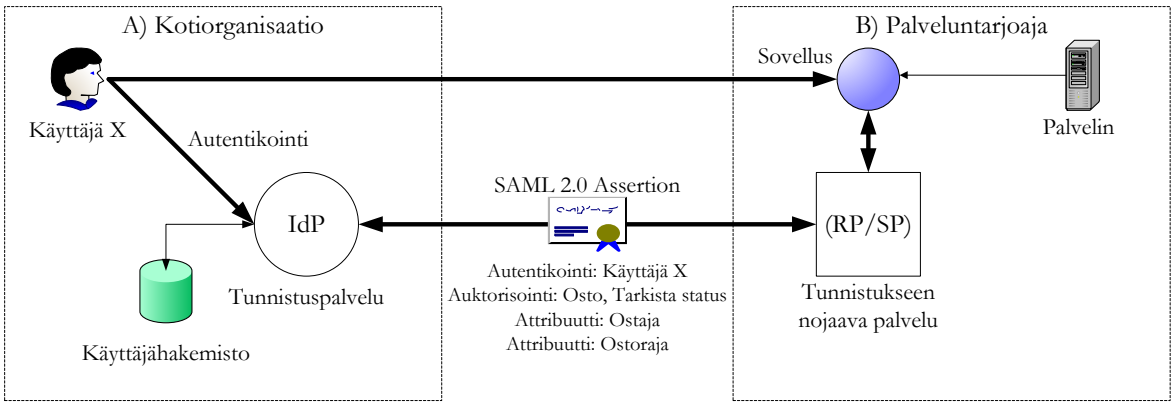
Organisaatiorajat ylittävässä identiteetinhallinnassa on kyse siitä, että eri organisaatiot muodostavat luottamukseen perustuvia kumppanuuksia keskenään. Kumppanuudet perustuvat sopimuksiin käyttäjien identiteettiin liittyvien tietojen jakamisesta organisaatioiden tietojärjestelmien välillä. Tästä luottamukseen perustuvasta konseptista käytetään termiä federoitu identiteetinhallinta. Perinteisesti autentikoinnin ja käyttövaltuuksien toiminnot on rakennettu kiinteästi sovelluksiin. Federoidun identiteetinhallinnan perusperiaate on se, että sovelluksissa luotetaan verkkopalvelujen rajapintojen kautta saataviin standardoituihin viesteihin. Määrämuotoiset viestit sisältävät autentikoinnin ja valtuutuksen määrittelevät tiedot. (Linden 2009, 43.)

Federoidun identiteetinhallinnan perustoiminnot (kuvio 1) ovat tunnistuspalvelu (Identity Provider, IdP) ja tunnistukseen nojaava palvelu (Service Provider, SP). Identity Provider on palvelu, joka tunnistaa käyttäjän ja sisältää ajantasaiset tiedot käyttäjän identiteetistä sekä siihen liittyvistä attribuuteista. Service Provider on tunnistukseen luottava palvelu, joka käyttää sovellusten pääsynvalvonnassa tunnistuspalvelusta saatuja attribuutteja. (Linden 2009, 44.)

Tällä hetkellä Security Assertion Markup Language (SAML) on vallitseva standardi federoidun identiteetinhallinnan tiedonvälityksessä. SAML perustuu XML-viesteihin eri organisaatioiden välillä. XML (Extensible Markup Language) on rakenteinen merkintäkieli, joka ei ole sidottu minkään tietyn ohjelmiston tai teknisen alustan käyttöön. Tämän johdosta se soveltuu hyvin eri organisaatioiden välisen tiedonvälitykseen toimintoihin federoidun identiteetinhallinnan toteutuksissa. (Boyle & Panko 2014, 322.)

SAML 2.0 standardin mukaan federoitu identiteetinhallinta sisältää keskeisenä toimintona väittämiin perustuvan autentikoinnin ja auktorisoinnin sekä tiedonvälityksen toiminnot. Väittämä sisältää sellaista tietosisältöä organisaatiosta A, että organisaation B tulisi luottaa tietosisältöön, mikäli organisaatioiden A ja B välillä vallitsee luottosuhde. Väittämien kolme keskeisintä elementtiä ovat autentikointiin, auktorisointiin ja attribuutteihin liittyvät tietosisällöt. Väittämissä voidaan välittää tietoa siitä, minkä niminen henkilö on autentikoitunut, millainen rooli hänellä on kotiorganisaatiossaan, ja mitä

muita attribuutteja hänen rooliinsa liittyy. Väittämien sisältämien tietojen pohjalta organisaatio B voi antaa oikeuksia tietojärjestelmiinsä, vaikka autentikointi on suoritettu organisaatiossa A. Organisaatioiden A ja B välillä ei siirretä salasanoihin tai käyttäjätunnuksiin liittyviä tietoja. (Boyle & Panko 2014, 321.)



Kuvio 1. Federoinnin periaate (Linden 2012, 52 ja Boyle & Panko 2014, 321)

Seitsosen ja Haukilehdon (6.3.2013) mukaan Microsoftin merkittävä tuote federoidun identiteetinhallinnan ratkaisuihin on Active Directory Federation Services (AD FS). Tuote tukee SAML-protokollaa toukokuussa 2010 julkaistusta AD FS 2.0 versiosta lähtien. Microsoft käyttää hieman erilaisia federoidun identiteetinhallinnan termejä ja dokumenteissa puhutaan claim-pohjaisesta todennuksesta sekä valtuutuksesta. Seuraavassa taulukossa on esitetty Microsoft termien ja SAML termien vastaavuus:

Taulukko 1. Termistöt ja yhteensopivuus (Seitsonen & Haukilehto 2013)

Konsepti	**Microsoft termi**	**SAML 2.0 termi**
Käyttäjää kuvaava XML dokumentti, jonka identiteettejä ylläpitävä osapuoli lähettää sovellusta hallitsevalle osapuolelle käyttöpyynnön aikana.	Security Token	Assertion
Käyttäjille Security Token viestejä luova osapuoli	Claims Provider (CP)	Identity Provider (IdP)
Security Token viestejä sovelluksen valtuutuksessa hyödyntävä osapuoli	Relying Party (RP)	Service Provider (SP)
Security Tokenin mukana lähetettävä data, joka kuvaa käyttäjää ja käyttäjän ominaisuuksia	Claim	Assertion statement

Federoidun identiteetinhallinnan ratkaisuja on kehitetty Suomessa ensimmäisenä yliopistojen ja korkeakoulujen käyttöön HAKA-luottamusverkoston muodossa. HAKA luottamusverkko on yliopistojen, korkeakoulujen ja tutkimuslaitosten sekä näitä palvelevien yhteisöjen luottamusverkko. Luottamusverkosto tarjoaa käyttäjätietoja palveluille SAML-määritysten mukaisesti, ja niiden avulla tarjotaan HAKA-käyttäjätunnistusjärjestelmä noin 296 000 loppukäyttäjälle. (CSC 2014.)

Valtion tieto- ja viestintätekniikkakeskus Valtori tarjoaa valtionhallinnon organisaatioiden käyttöön Virtu-palvelua. Virtu on virkamiehen kertakirjautumisratkaisu, joka perustuu federoituun identiteetinhallintaan. Virtu-palvelun avulla on mahdollista toteuttaa kertakirjautumisen toiminnot niihin selainpohjaisiin järjestelmäpalveluihin, joita valtionhallinnossa käytetään. Palveluun liittynyt organisaatio voi myös toteuttaa oman IdP-palvelimen toiminnot Virtu-palvelun avulla. (Valtori 2014.)

3.3 Käyttäjäkeskeinen hallintataso

Työantajan näkökulmasta käyttäjillä on vahva sidos organisaatioon ja siellä käytettäviin tietojärjestelmiin. Tällöin sähköisen identiteetin attribuuttien oikeellisuus ja ajantasaisuus sekä tunnistuspalvelujen toimivuus ovat organisaatioille tärkeitä toiminnollisuuksia. Käyttäjäkeskeinen federoitu identiteetinhallinta on organisaatioiden toimintaan sidotun federoidun identiteetinhallinnan vastakohta. (Linden 2012, 58.)

Jos näkökulma siirretään käyttäjään, niin henkilöllä voi olla käytössään useita sähköisiä identiteettejä, jotka voivat olla myös globaaleja (esim. Yahoo tai Google tunnus). Tällöin tilanne voidaan kääntää toisinpäin ja henkilön luoma globaali identiteetti (esim. Google tunnus) voikin toimia tunnisteena kirjauduttaessa myös organisaation tietojärjestelmiin. Käyttäjäkeskeisen identiteetinhallinnan keskeinen ominaisuus on kuitenkin se, ettei kukaan voi taata identiteettiin liittyvien attribuuttien luotettavuutta. Menetelmän tarkoitus ei olekaan tarjota vahvaa identiteettiä, vaan sen tarkoitus on poistaa käyttäjien velvoite rekisteröityä erikseen eri palveluihin. Tunnetuin teknologia käyttäjäkeskeiseen identiteetin hallintaan on OpenID-tunnistuspalvelu. (Linden 2012, 59.)

3.4 Kertakirjautuminen

SSO (Single Sign On) eli kertakirjautuminen on erillinen konsepti suhteessa hallintatasoihin. Kertakirjautumisen yleisin käyttökohde on organisaatioiden sisällä, jolloin käytetään myös termiä ESSO (Enterprise Single Sign On). Kertakirjautuminen voidaan toteuttaa myös useiden organisaatioiden välillä, jolloin SSO toiminnollisuus ylittää organisaatiorajat (multidomain SSO). SSO voidaan järjestää myös siten, että kertakirjautuminen tehdään verkon yli selaimella kirjautumalla (Web-based SSO). Kertakirjautumisen tärkein ominaisuus on se, että käyttäjän tarvitsee suorittaa kirjautuminen vain kerran ja sen jälkeen autentikointi on voimassa koko käyttösession ajan, niin kauan kunnes käyttäjä kirjautuu ulos tai istunto katkeaa yhteyden katkeamisen vuoksi. (Bertino & Takahashi 2011, 55.)

Lindenin (2012, 27) mukaan kertakirjautuminen voidaan jakaa **näennäiskertakirjautumiseen** (pseudo single sign-on) ja **aitoon kertakirjautumiseen** (true single sign-on). Näennäiskertakirjautuminen toimii siten, että väliohjelmistoon tallennetaan käyttäjätunnukset ja salasanat istunnon alussa. Käyttäjä kirjautuu istunnon alussa pelkästään väliohjelmistoon, joka taas huolehtii kirjautumisesta autentikointipalvelimen kanssa tarpeen niin vaatiessa. Aidossa kertakirjautumisessa on myös käytössä väliohjelmisto, mutta siinä ei tallenneta välivarastoon käyttäjätunnuksia ja salasanoja. Väliohjelmisto toimii siten, että käyttäjän kirjautumisen jälkeen palvelut luottavat väliohjelmiston tuottamiin käyttäjän identiteetin todentaviin tunnistussanomiin (ticket assertion).

Microsoftin Windows palvelinarkkitehtuurin toimialuekirjautumisen yhteydessä Kerberos protokolla tarjoaa aidon kertakirjautumisen organisaation sisällä. Kerberos autentikointiprotokolla käyttää salakirjoitustekniikkaa ja menetelmä täyttää siten myös vahvan autentikoinnin määritelmän. Nykyään Kerberos protokollasta käytetään vuonna 1993 luotua versiota 5. (Linden ym. 2011, 78.)

4 Kohdeorganisaation kuvaus

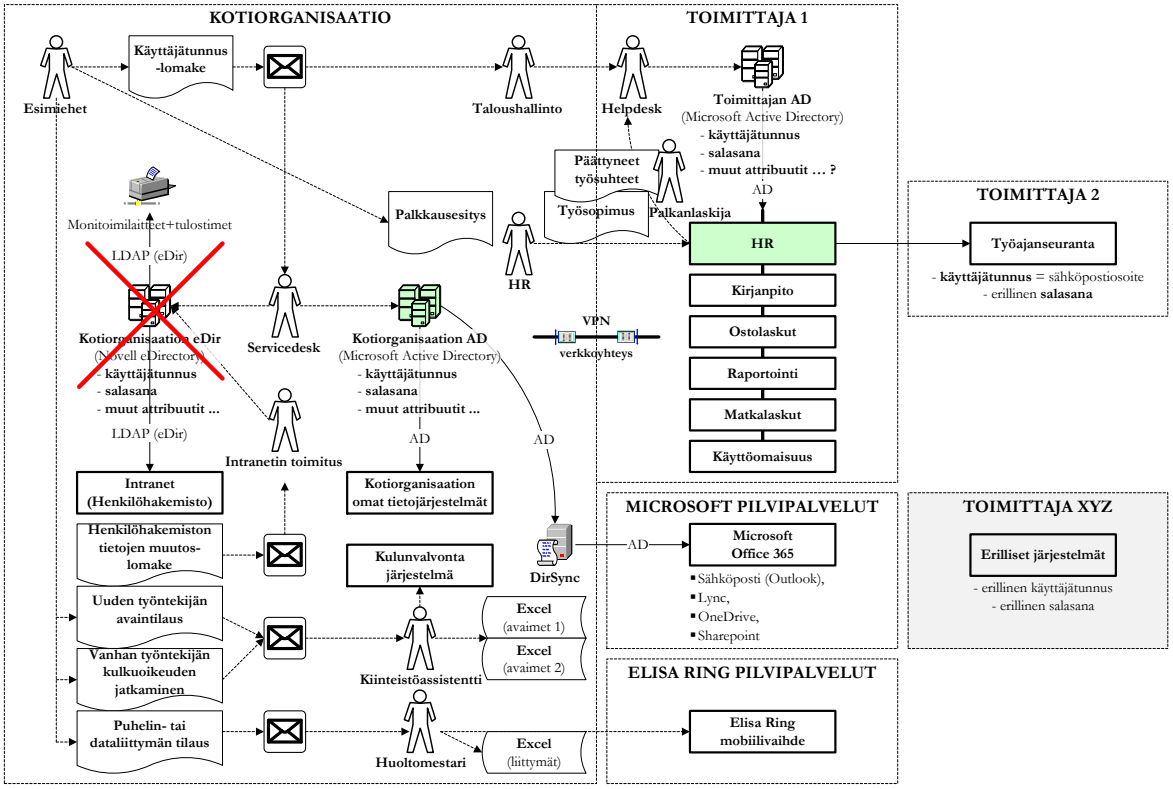
Kohdeorganisaatio ja opinnäytetyön toimeksiantaja on julkishallinnon organisaatio, jossa on noin 250 työntekijää. Toiminta on jakautunut useaan erilliseen rakennukseen, joiden välille on rakennettu toimipaikat yhdistävä yhteinen tietoverkko. Organisaatio muodostuu useasta eri osastosta, joiden alla on useita eri yksiköitä. Tietohallinto on matriisiorganisaation mukaisena toimintona keskitetty ja tietohallintoyksikkö tarjoaa palveluja kaikille organisaation osastoille.

Suuri muutos tietojärjestelmissä tapahtui vuodenvaihteessa 2013 – 2014, jolloin organisaatiomuutoksen yhteydessä otettiin käyttöön uudet talous- ja henkilöstöhallinnon tietojärjestelmät SaaS-ostopalveluna.

4.1 Nykytilan kuvaus

Toimeksiantajan tietojärjestelmien osalta palvelut siirtyvät yhä enemmän verkkoon ja ohjelmistojen tarjoaminen verkossa palveluna sekä pilvipalvelut yleistyvät voimakkaasti. Palvelujen tekninen alusta hankitaan usein kokonaan ostopalveluna ja itse ylläpidetään vain välttämättömät sisäiset palvelut omilla palvelimilla. Myös omien palvelimien konesalipalvelut hankitaan tulevaisuudessa pääosin ulkoistettuna ja palvelimia käytetään sekä ylläpidetään omin voimin verkon yli toimittajan hallinnoimassa konesalissa.

Toimeksiantajan organisaatiossa on käytössä lukuisia tietojärjestelmiä sekä omassa tietoverkossa, että ulkoistetuilla toimittajilla. Havaittujen ongelmatilanteiden perusteella on todettu tarve kehittää tietojärjestelmien pääsynvalvonnan ja käyttöoikeuksien hallinnan työprosesseja sekä työkaluja. Nykytilan selvityksen perusteella on muodostettu kokonaiskuva tilanteesta (kuvio1).



Kuvio 2. Kohdeorganisaation nykytilan kuvaus

Nykytilan ongelmakentän eri osat muodostuvat seuraavissa kappaleissa kuvatuista tietojärjestelmistä ja niihin liittyvistä pääsyn- ja käyttövaltuushallinnan prosesseista.

Organisaation oma autentikoinnin käyttäjähakemisto on siirtymässä pelkästään Microsoft Active Directoryn käyttöön. Vanha Novell eDirectory hakemistopalvelu on poistumassa käytöstä ja siihen kytketyt käyttäjähakemistopalvelut siirretään Active Directoryyn. Viimeisiä siirrettäviä palveluja ovat intranetin ja Servicedesk-ohjelmiston sekä monitoimilaitteiden ja verkkokirjoittimien autentikointi. Molemmissa hakemistopalveluissa on käytössä LDAP-rajapinta. Merkittävä eDirectoryyn kytketty sovellus on intranetin yhteydessä sijaitseva henkilöhakemistosovellus. Henkilöhakemisto sisältää perustiedot kaikista työntekijöistä ja heidän tehtävistään organisaatiossa.

Henkilöstöhallinnon järjestelmä on hankittu SaaS-ostopalveluna ja sen autentikointi on liitetty toimittajan Active Directory hakemistopalveluun. Tietojärjestelmässä säilytetään henkilöstön palkkaukseen ja työsuhteeseen liittyviä tietoja. Esimiehet tekevät palkkausehdotuksen, joka toimitetaan henkilöstöhallintoon johtajien hyväksynnän jälkeen.

Henkilöstöhallinto tekee työsopimuksen ja työsopimuksen perusteella palkanlaskija tekee pyynnön toimittajan Helpdeskiin, jolloin uusi käyttäjätunnus luodaan. Toimittajan Helpdesk määrittelee tietojärjestelmään käyttäjäroolit sen perusteella, onko käyttäjä esimies vai työntekijä, ja mihin yksikköön hän kuuluu. Työsuhteen päättyessä henkilöstöhallinto toimittaa tiedot palkanlaskentaan. Palkanlaskija toimittaa kerran kuukaudessa tiedot päättyneistä työsuhteista toimittajan Helpdeskiin, jolloin tunnus poistetaan. Järjestelmän pääkäyttäjien tunnukset on luotu käyttöönoton yhteydessä ja ne muuttuvat harvoin. Mahdolliset muutokset pyydetään toimittajan Helpdeskistä. Tunnisteita järjestelmässä ovat käyttäjätunnus, sähköpostiosoite ja henkilönumero.

Taloushallinnon järjestelmät on hankittu SaaS-ostopalveluna ja niiden autentikointi on liitetty toimittajan Active Directory hakemistopalveluun. Tietojärjestelmissä säilytetään kirjanpitoon, ostolaskuihin, raportointiin, matkalaskuihin ja käyttöomaisuuteen liittyviä tietoja. Esimiehet tekevät Servicedeskin käyttäjätunnuslomakkeen avulla uuden työntekijän tunnuksen perustamispyynnön. Lomake sisältää valinnan ostolaskujen ja matkalaskujen järjestelmiin pääsystä. Lomake toimitetaan Servicedeskin postilaatikkoon ja samalla taloushallinnon yhteiskäyttöiseen postilaatikkoon. Taloushallinto tarkistaa käyttöoikeuspyynnön ja muuttaa sitä tarvittaessa. Tarkistuksen jälkeen taloushallinto välittää pyynnön sähköpostilla toimittajan Helpdeskiin. Toimittajan Helpdesk määrittelee tietojärjestelmään käyttäjäroolit taloushallinnon määrittelyjen mukaisesti. Toimittajan Helpdesk poistaa tunnukset taloushallinnon pyynnön mukaisesti. Järjestelmän pääkäyttäjien tunnukset on luotu käyttöönoton yhteydessä ja ne muuttuvat harvoin. Mahdolliset muutokset pyydetään toimittajan Helpdeskistä. Tunnisteita järjestelmissä ovat käyttäjätunnus, sähköpostiosoite ja henkilönumero.

Microsoftin Office 365 pilvipalvelu on hankittu organisaatiomuutoksen yhteydessä vuoden 2013 loppupuolella. Palvelu sisältää sähköposti-, kalenteri-, pikaviesti-, pilvitallennus- ja ryhmätyöpalvelut. Palvelun autentikointi on liitetty organisaation omaan Active Directory hakemistopalveluun Microsoftin DirSync (Directory Synchronization) työkalun avulla. Esimiehet tekevät Servicedeskin käyttäjätunnuslomakkeen avulla uuden työntekijän tunnuksen perustamispyynnön. Lomake toimitetaan Servicedeskin postilaatikkoon ja käyttäjälle tehdään uusi Active Directory tunnus lomakkeen tietojen pe-

rusteella. Lomake sisältää tiedot myös käyttövaltuuksien määrittelyyn roolien perusteella. Tunnuksen perustamisen yhteydessä luodaan käyttäjälle myös tarvittaessa postilaatikko ja tiedot siirtyvät Office 365 palveluun DirSync työkalun avulla. Tieto käyttöoikeuden päättymisestä tulee vaihtelevasti ilman määrämuotoista menettelyä. Servicedesk poistaa tunnuksen järjestelmästä saatuaan tiedon. Tunniste järjestelmään on Active Directoryn userprincipalname, joka on käyttäjätunnus@domain.fi tyyppinen käyttäjätunnus.

Mobiilivaihde ja puhelinjärjestelmä on hankittu organisaatiomuutoksen yhteydessä vuoden 2013 loppupuolella. Palvelu sisältää mobiilivaihteen pilvipalveluna. Tunnusten autentikointi on liitetty toimittajan Active Directory hakemistopalveluun. Kiinteistöhallinnon huoltomestari saa puhelin ja dataliittymän tilauksen osastojen yhteyshenkilöiltä. Huoltomestari tekee mobiilivaihteeseen liittymän ja syöttää identiteetin perustiedot, joita ovat etunimi, sukunimi ja sähköpostiosoite jos sellainen on. Tieto käyttöoikeuden päättymisestä tulee vaihtelevasti ilman määrämuotoista menettelyä. Huoltomestari poistaa liittymän järjestelmästä saatuaan tiedon. Tunnisteita järjestelmässä ovat palvelun oma käyttäjätunnus ja puhelinnumero.

Kulunvalvonnan järjestelmä on vaihtumassa ja nykyinen ratkaisu muuttuu uuteen järjestelmään. Nykyinen ratkaisu on sisältänyt myös työajan seurannan toiminnot, mutta työajanseurantaan tulee uusi tietojärjestelmä. Uuden järjestelmän autentikointi on erillinen, eikä sitä ole liitetty muihin organisaation järjestelmiin. Esimiehet tekevät intranetin avaintunnuslomakkeen avulla uuden työntekijän avainten hankinnan eli kulunvalvonnan tunnuksen perustamispyynnön. Nykyisen kulkuoikeuden jatkosta on erillinen lomake intranetissä. Lomake toimitetaan yhteiskäyttöiseen AvainTilaus postilaatikkoon. Kiinteistöhallinnon kiinteistöassistentti tekee lomakkeen perusteella tunnukset kulunvalvonnan järjestelmiin ja määrittelee kulkuoikeudet. Tieto kulkuoikeuden päättymisestä tulee vaihtelevasti ilman määrämuotoista menettelyä. Kiinteistöassistentti poistaa tunnuksen järjestelmästä saatuaan tiedon. Tunnisteita järjestelmissä ovat avaintunnus ja henkilönumero.

Työajanseurannan järjestelmä on vaihtumassa ja nykyinen järjestelmä muuttuu uudeksi. Järjestelmän autentikointi on erillinen, mutta käyttäjätunnusten ja roolien siirto

on integroitu henkilöstöhallinnon järjestelmään. Käyttäjätiedot siirtyvät automaattisesti henkilöstöhallinnon järjestelmästä. Tunnukset syntyvät ja poistuvat HR-järjestelmän tietojen ohjaamina. Autentikoinnin tunnuksena toimii käyttäjätunnus, salasana on erillinen. Käyttövaltuudet määrittyvät HR-järjestelmästä siirtyvän tiedon perusteella. Tunnisteita järjestelmässä ovat käyttäjätunnus, sähköpostiosoite ja henkilönumero.

4.2 Nykytilan analyysi

Toimeksiantajan tietoverkossa on käytössä lukuisia erilaisia käyttäjätunnus ja salasana yhdistelmiä eri tietojärjestelmiin. Tietojärjestelmien käyttäjiin liittyvää tietoa säilytetään useissa erillisissä rekistereissä ja niiden hallintaan sovelletaan erilaisia menetelmiä eri vastuuhenkilöiden toimesta. Tiedoissa on päällekkäisyyksiä ja tietojen muutokset eivät aina välity eri osapuolten välillä. Käyttäjätunnusten ja henkilöihin liittyvien tietojen elinkaaren hallinnassa on turhia manuaalisia välivaiheita, joita voidaan poistaa parantamalla työkaluja ja toimintaprosesseja. Toimintaprosessit ovat eriytyneet ja kokonaiskuva on ollut puutteellinen. Prosessien kuvaaminen ja tavoitetilan suunnittelu ovat tärkeitä toimenpiteitä.

Tunnusten ja käyttövaltuuksien perustaminen tapahtuu määrämuotoisen menettelyn kautta ja siinä noudatetaan olemassa olevaa prosessia. Perustamispyynnöistä jää lokitiedot sähköpostijärjestelmiin ja pyynnöt tehdään sähköisillä lomakkeilla. Poikkeuksena ovat puhelinliittymien tilaukset, jotka tapahtuvat suullisesti tai sähköpostin välityksellä. Henkilöstöhallinnon tietojärjestelmään tunnukset perustetaan työsopimusten kautta ja tunnusten poistaminen tapahtuu sopimuksen päättymisen perusteella.

Käyttövaltuuksien jatkamiseen on olemassa määrämuotoinen prosessi ja muutospyynnöt kulkevat sähköisten lomakkeiden kautta. Pitkien vapaiden ja poissaolojen osalta tiedot eivät aina kulkeudu järjestelmiin. Sähköiseen identiteettiin liittyvien tietojen muutoksissa on viiveitä ja manuaalisia välivaiheita. Tietojen muutoksia täytyy pyytää lomakkeella tai sähköpostilla ja varsinaisen muutoksen tekee henkilö, jolla on työkalut ja käyttövaltuudet Active Directoryyn tai eDirectoryyn. Kahden käyttäjähakemiston ylläpito omassa kotiorganisaatiossa aiheuttaa turhaa työtä ja toisesta tulisi päästä eroon mahdollisimman nopeasti.

Tunnusten ja käyttövaltuuksien poistoon ei ole olemassa määrämuotoista prosessia, joka kattaisi kaikki osa-alueet. Henkilöstöhallinnon osalta prosessi on olemassa ja sille on määritelty selvät vastuut ulkopuolisen toimittajan kanssa. Tietojen välittyminen työsuhteiden päättymisestä kotiorganisaation omille toimijoille on kuitenkin puutteellista ja muihin järjestelmiin voi jäädä voimaan tunnuksia henkilöille, jotka eivät ole enää organisaation palveluksessa.

Käyttäjätunnusten autentikointi ei ole keskitetty vain yhteen käyttäjähakemistoon, vaan käytössä on useita eri käyttäjähakemistoja. Vallitseva tilanne johtaa useisiin eri tunnus ja salasana yhdistelmiin. Tietojärjestelmien lisääntyessä autentikoinnin keskittäminen yhteen käyttäjähakemistoon on tarpeellinen kehityshanke. Nykyisessä toiminnassa salasanojen vaihtamista ei ole pakotettu säännöllisesti. Tilanne on jäänyt uusien järjestelmien käyttöönottovaiheessa sovittuun tilaan, jolloin vaihtopakko oli poistettu. Tietoturvan kannalta salasanojen vaihto tulee järjestää suositusten mukaan vähintään 90 päivän välein (Boyle & Panko 2014, 280). Mikäli käytössä on useita eri käyttäjähakemistoja yhtä aikaa, joutuvat käyttäjät vaihtamaan salasanoja useisiin eri paikkoihin moneen kertaan.

5 Kehittämissuunnitelma

Lindenin mukaan (2012, 8-9) identiteetin- ja pääsynhallinnan kehittämisessä haasteet eivät suinkaan ole pelkästään tietoteknisiä ongelmia. Merkittävä osuus työstä on kohdennettava organisaation toimintaprosessien mallintamiseen ja kehittämiseen kohti määrämuotoista ja kurinalaista toimintamallia. Kehittämisprojektissa on tärkeätä tunnistaa oleelliset kehittämiskohteet ja pystyä priorisoimaan niiden toteutusjärjestys. Kehittämistoimenpiteiden vaiheittainen toteuttaminen on siis suositeltavaa.

Kohdeorganisaatiossa perustettiin projekti, jonka tavoitteena oli organisaation pääsyn- ja käyttövaltuushallinnan kehittäminen. Projektiryhmän keskeinen tehtävä oli nykyisten toimintaprosessien kuvaaminen ja niiden kehittäminen havaittujen puutteiden pohjalta. Prosessikuvaukset jaettiin kolmeen pääkategoriaan, jotka olivat tunnusten sekä käyttövaltuuksien perustaminen, muutos ja poistaminen.

Toiseksi tärkeäksi kehittämistavoitteeksi todettiin yhteen keskitettyyn hakemistopalveluun siirtyminen. Tavoitteena on, että yhteen keskitettyyn hakemistopalveluun ja sen käyttäjähakemistoon tallennetaan kaikki käyttäjien sähköiseen identiteettiin liittyvät attribuutit. Sen jälkeen tiedot siirtyvät automatisoidusti mahdollisimman moneen eri organisaation käyttämään tietojärjestelmään ilman manuaalisia välivaiheita tai erillisiä rekistereitä. Keskittäminen ja tiedonsiirron automatisointi vähentävät tulevaisuudessa työresurssien käytön tarvetta eri välivaiheissa.

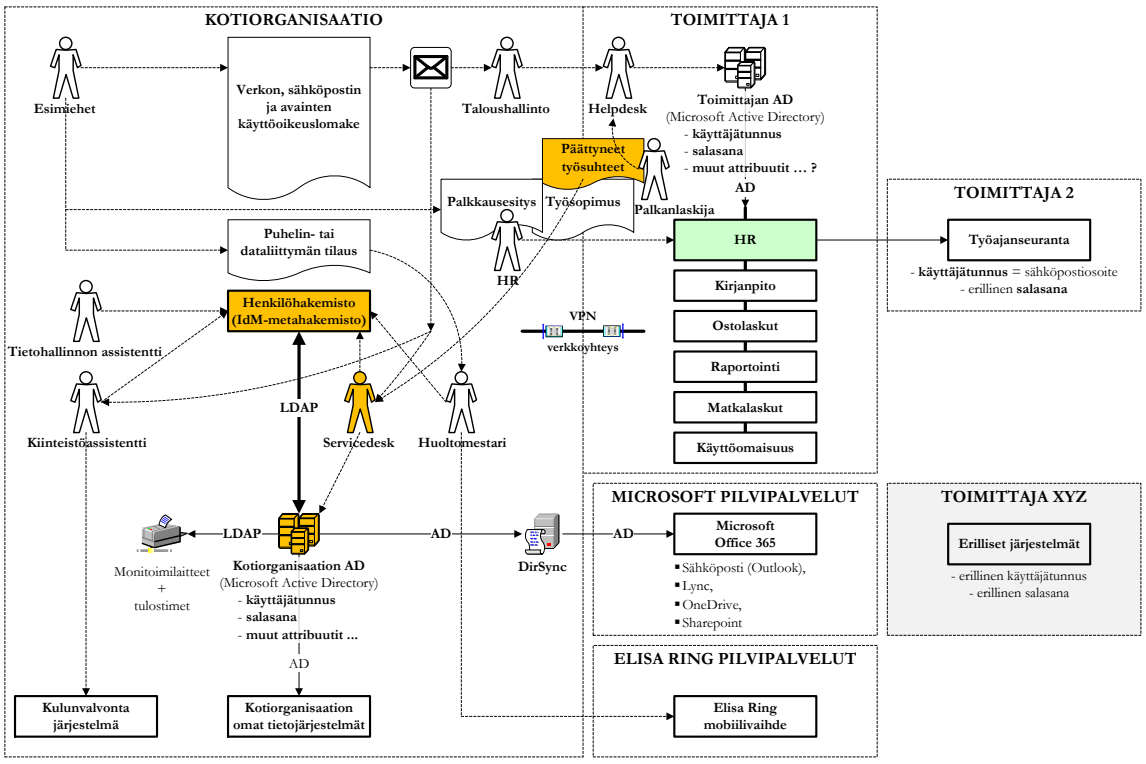
Kolmas priorisoitu kehityskohde on uuden henkilöstöhakemiston sovelluksen kehittäminen. Nykyisen sovelluksen elinkaarta ei voi enää jatkaa, koska sovellusta ei ylläpidetä. Lisäksi pian siirrytään käyttämään vain yhtä käyttäjähakemistoa. Muutoksen yhteydessä sidokset vanhaan käyttäjähakemistoon täytyy purkaa kaikista siihen liitetyistä tietojärjestelmistä. Kehitettävän sovelluksen vaatimuksena on, että sillä pitää pystyä selaamaan sekä muokkaamaan käyttäjien tietoja suoraan siten, että tiedot siirtyvät Active Directory hakemistoon.

Tulevaisuudessa toteutettaviksi kehitystoimenpiteiksi jäävät organisaation tietohallinnon federoidun identiteetinhallinnan osaamisen kehittäminen ja tarpeellisten työkalujen

käyttöönotto, sitten kun riittävät valmiudet siihen ovat olemassa. Federointi vaatii sopimista ja yhteistyötä sekä teknisiä valmiuksia myös niiden kumppaneiden kanssa, jotka ylläpitävät sovelluksia SaaS-palveluna.

Kehittämissuunnitelman ensimmäisen vaiheen tavoitetilan kuvaus on esitetty kuviossa 3. Tavoitetilassa kotiorganisaatiossa on otettu käyttöön kehitetyt määrämuotoiset prosessit ja siirrytty käyttämään pelkästään Microsoft Active Directory hakemistopalvelua käyttäjien keskeisenä autentikoinnin lähteenä. AD-hakemistoon tallennetaan myös käyttäjiin liittyvät keskeiset tiedot eli sähköisen identiteetin attribuutit.

Uusittu henkilöhakemistosovellus toimii organisaation sisäisenä henkilöhakemistona sekä tietojen ylläpidon sovelluksena. Käyttäjiin liittyviä tietoja voidaan ylläpitää helposti selainkäyttöisellä sovelluksella hajautetusti tietojen ylläpitäjien toimesta. Henkilöhakemistosta on myös linkki uusittuun käyttäjätunnuslomakkeeseen, joka sisältää samassa lomakkeessa kulkuoikeuksien pyytämiseen ja jatkamiseen liittyvät tiedot. Tällöin esimiesten ei tarvitse käyttää useita eri lomakkeita valtuuksien pyynnöissä.

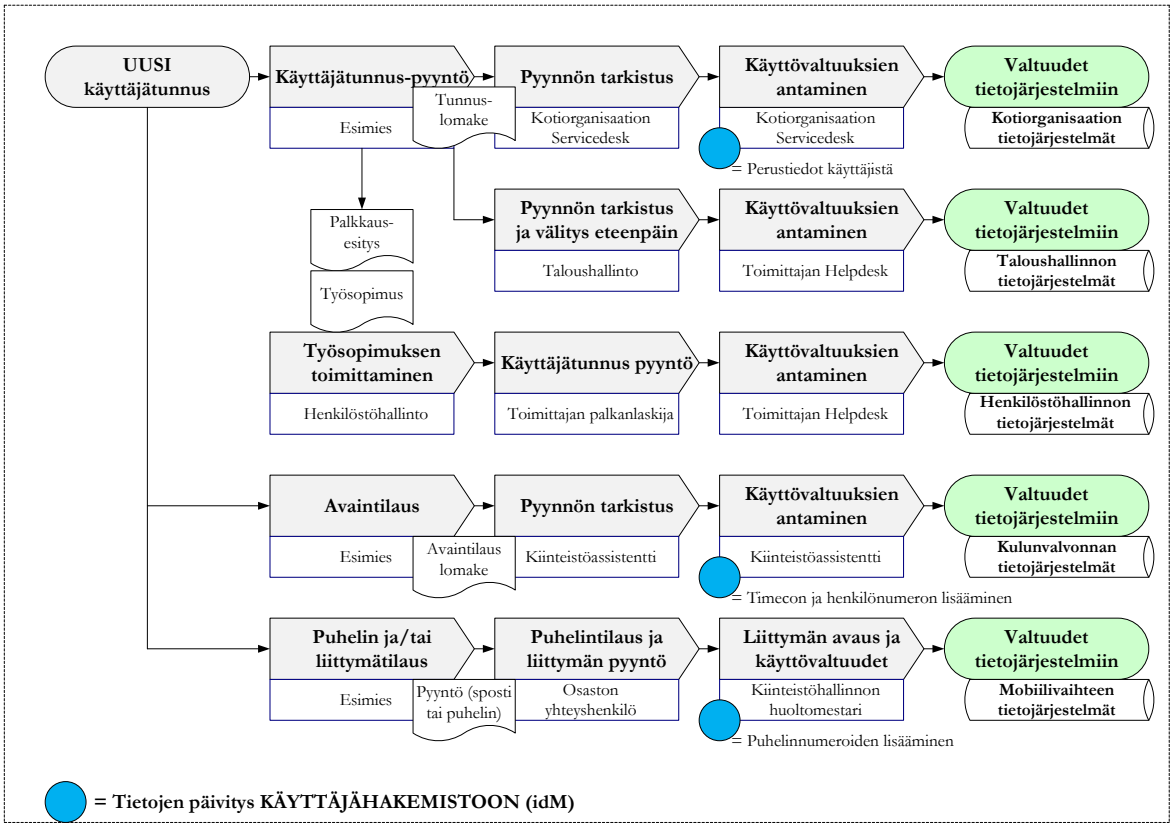


Kuvio 3. Kohdeorganisaation ensimmäisen vaiheen tavoitetilan kuvaus

5.1 Määrämuotoisten prosessien kehittäminen

Käyttäjätunnusten ja käyttövaltuuksien perustamisen prosessit selvitettiin ja tavoitetila kuvattiin projektiryhmän työskentelyssä (kuvio 4). Tunnusten perustamisen pyynnöt etenevät määrämuotoisen menettelyn kautta ja esimiesten täyttämien lomakkeiden ja palkkausesitysten myötä tarvittaviin tietojärjestelmiin perustetaan uusille käyttäjille tunnukset sekä annetaan tarvittavat käyttövaltuudet.

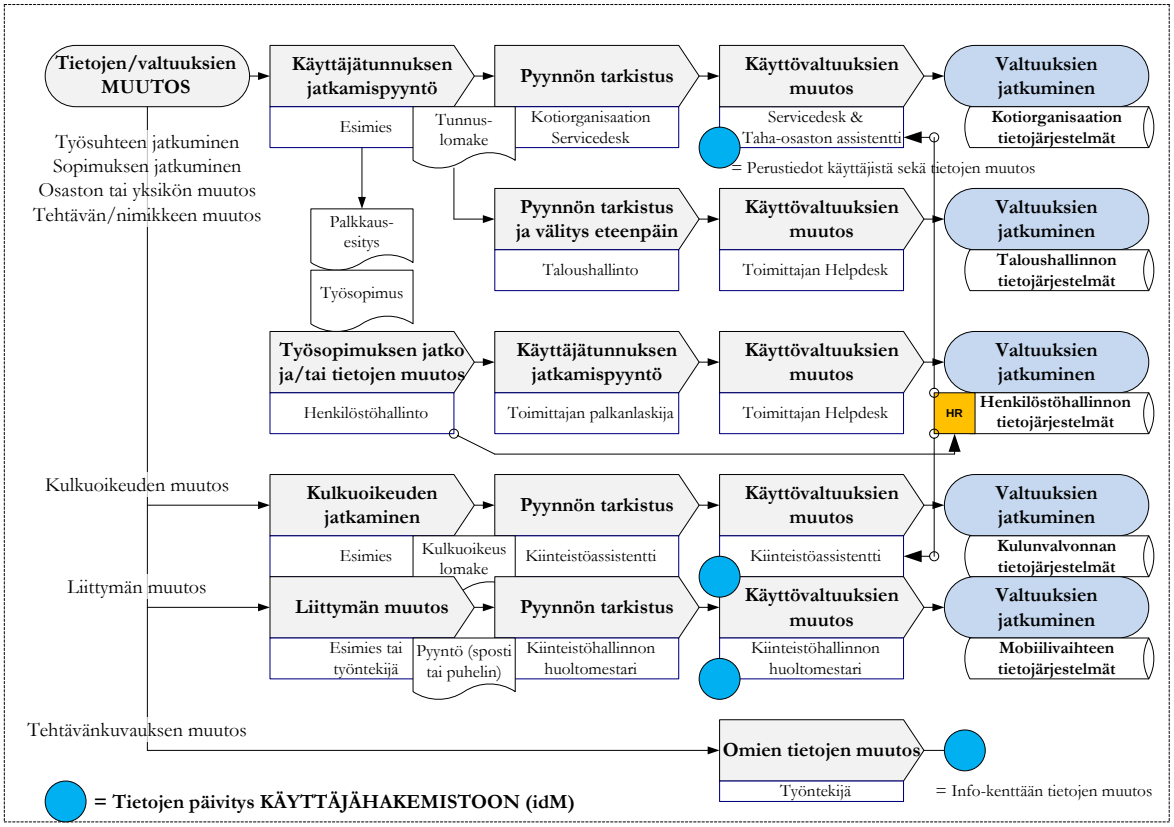
Käyttäjätunnuksin liittyvät lisätiedot tulee kirjata organisaation omaan Active Directory käyttäjähakemistoon heti siinä vaiheessa kun tiedot ovat selvillä. Käyttövaltuuksien perustamisen yhteydessä Servicedesk kirjaa käyttäjistä perustiedot, joita ovat nimi, nimike, osasto, sähköposti ja puhelinnumerot jos ne ovat tiedossa. Jos puhelinnumerot selviävät vasta tunnuksen perustamisen jälkeen, niin huoltomestari kirjaa tiedot itse suoraan käyttäjähakemistoon. Kiinteistöassistentti kirjaa tiedot kulunvalvonnan tunnisteesta ja henkilönumerosta. Henkilönumero saadaan poimittua uudesta työajanseurannan järjestelmästä, joka on suoraan yhteydessä HR-järjestelmään. Uuden henkilöhakemistosovelluksen avulla ylläpitäjät voivat suoraan muuttaa käyttäjähakemiston tietoja.



Kuvio 4. Uuden tunnuksen perustaminen, prosessikuvaus

Käyttövaltuuksien tai tietojen muutosten prosessit selvitettiin ja tavoitetila kuvattiin projektiryhmän työskentelyssä (kuvio 5). Muutosten pyytämiseen oli olemassa määrämuotoiset menettelytavat tunnusten ja kulkuoikeuksien jatkamisen osalta. Puhelinliittymä säilyi käytössä edelleen työsuhteen jatkuessa, joten siitä ei tarvittu erillistä ilmoitusta.

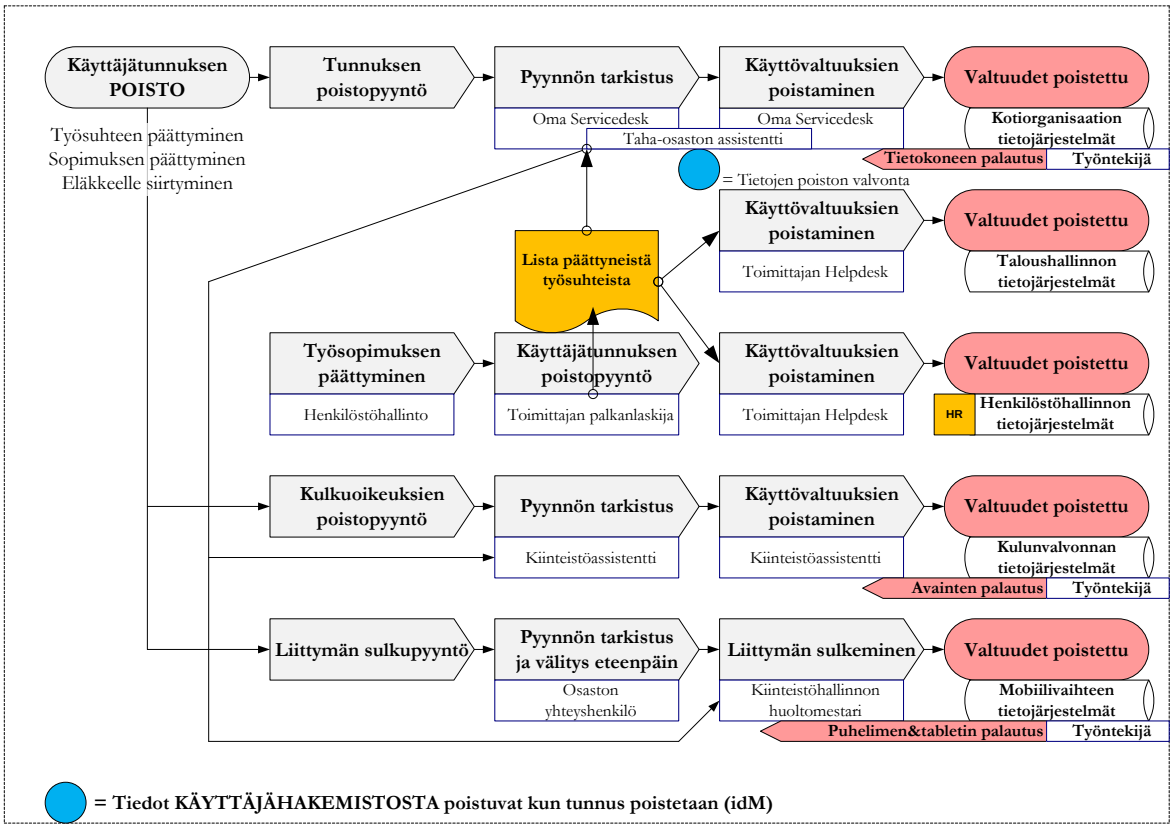
Tavoitetilan prosessiin on lisätty tarpeelliseksi todettu toiminnollisuus, jonka avulla henkilöstöhallinnon tietojärjestelmästä saadaan säännöllisin väliajoin listaus muuttuneista tiedoista. Tietojen muutos voidaan rajata omassa käyttäjähakemistossa tarvittaviin tietoihin, jolloin kaikista mahdollisista muutoksista HR-järjestelmässä ei tarvitse toimittaa tietoja muille osapuolille. Tarvittavat tiedot toimitetaan organisaation omaan Servicedeskiin ja kulunvalvonnan tietoja ylläpitävälle kiinteistöassistentille. Toimijat päivittävät muuttuneet tiedot käyttäjähakemistoon. Uuden henkilöhakemistosovelluksen avulla ylläpitäjät sekä käyttäjät itse voivat muuttaa käyttäjähakemiston tietoja määriteltyjen käyttövaltuuksien rajoissa.



Kuvio 5. Tietojen tai valtuuksien muutos, prosessikuvaus

Käyttövaltuuksien ja tunnusten poistamisen prosessit selvitettiin ja tavoitetila kuvattiin projektiryhmän työskentelyssä (kuvio 6). Tunnusten ja käyttövaltuuksien poistamisen prosessit olivat puutteelliset aikaisemmassa toimintamallissa. Tunnusten poistamiselle ei kaikilta osin ollut määrämuotoista menettelyä. Talous- ja henkilöstöhallinnon osalta poistoprosessit olivat melko hyvin kunnossa ja vastuuhenkilöt huolehtivat niiden toteutumisesta. Kotiorganisaation omille toimijoille tieto poistuneista työntekijöistä ei kuitenkaan kulkenut minkään vakiintunen prosessin mukaisesti.

Nykyisessä toimintamallissa toimittajan palkanlaskija toimittaa kerran kuukaudessa tiedot päättyneistä työsuhteista toimittajan Helpdeskiin, jolloin tunnus poistetaan. Tavoitetilan prosessiin lisättiin merkittävänä uutena toimintona tiedon toimittaminen säännöllisin väliajoin päättyneistä työsuhteista myös kotiorganisaation Servicedeskille.



Kuvio 6. Käyttäjätunnuksen poisto, prosessikuvaus

5.2 Henkilöhakemistosovelluksen uusiminen

Kohdeorganisaation nykyisessä intranetissä oleva henkilöhakemisto on koettu sisäisessä toiminnassa tärkeäksi ja sen haluttiin edelleen olevan käytössä uudistusten jälkeenkin. Henkilöhakemisto sisältää perustiedot kaikista työntekijöistä ja heidän tehtävistään organisaatiossa. Tietoihin on liitetty myös valokuva henkilöstä, jolloin sovellus toimii tärkeänä sisäisenä tietolähteenä. Sovellus on rakennettu Joomla julkaisujärjestelmän yhteyteen ja se on räätälöity PHP-sovellus, joka on integroitu Novell eDirectory käyttäjähakemistoon LDAP-rajapinnan avulla.

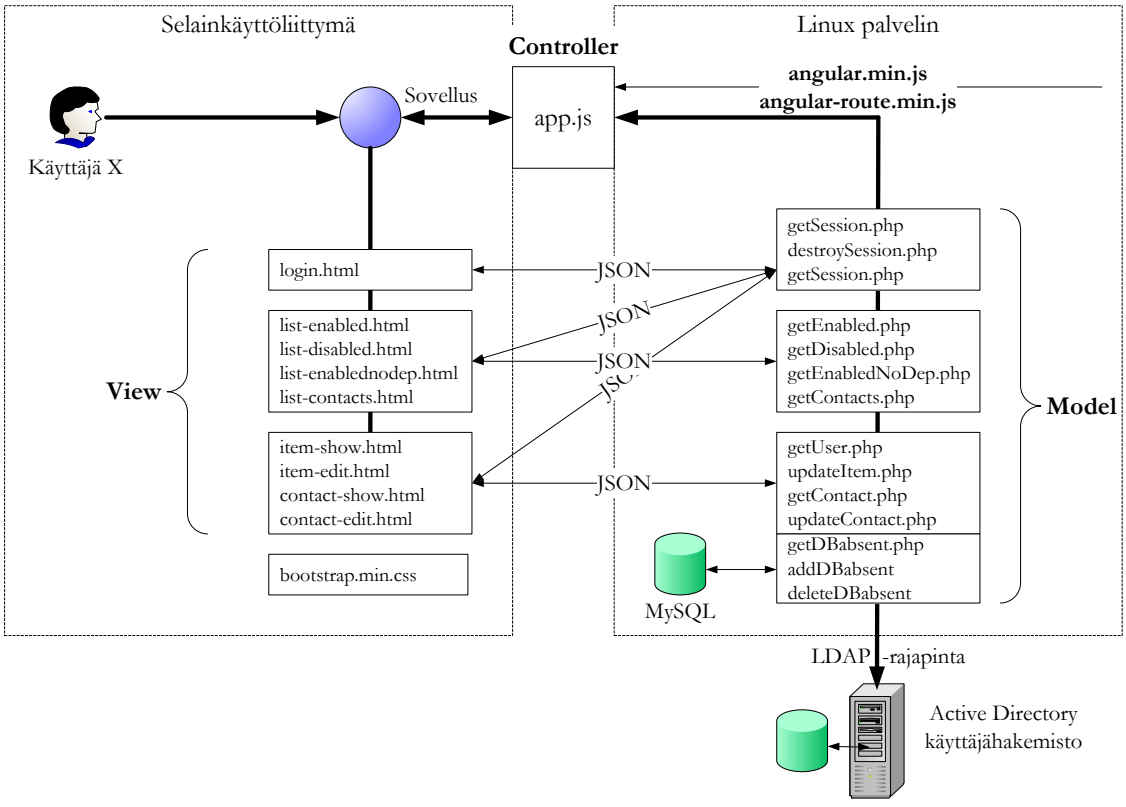
Ongelmaksi on muodostunut se, että aikoinaan sovelluksen rakentanut yritys ei enää ylläpidä sovellusta ja sovelluksen koodanneet ohjelmoijat eivät ole enää yrityksen palveluksessa. Sama yritys on myös räätälöinyt intranetin perustana toimivan Joomla julkaisujärjestelmän ja siitäkin ollaan siirtymässä pois, samoin kuin eDirectory on poistuva hakemistopalvelu.

Heti työn alkuvaiheessa todettiin, että nykyistä henkilöhakemistosovellusta ei pystytä ylläpitämään jatkossa ja sen tilalle täytyy saada uusi ratkaisu. Uuden ratkaisun tulisi olla integroitavissa suoraan organisaation omaan Active Directory käyttäjähakemistoon. Sovelluksen tulisi myös olla helposti liitettävissä organisaation tulevaan intranet ratkaisuun. Rajauksena on kuitenkin se, että sovellus on saavutettavissa vain organisaation sisältä palomuurilla suojatussa verkossa.

Opinnäytetyön yhteydessä rakennettiin vähimmäisvaatimukset täyttävä selainkäyttöinen sovellus. Sovelluksen käyttöliittymä ja logiikka on rakennettu Googlen kehittämällä AngularJS teknologialla, joka perustuu JavaScriptin toimintaan selainkäyttöliittymässä (AngularJS 2014). AngularJS käyttöliittymän komponentit ottavat yhteyden PHP-palvelimella sijaitseviin PHP-tiedostoihin, jotka käsittelevät LDAP-komennot Microsoft Active Directory hakemistopalvelun LDAP-rajapinnan välillä. Tiedonsiirto käyttöliittymän sivujen ja palvelimen PHP-tiedostojen välillä tapahtuu JSON-muodossa (JavaScript Object Notation).

Sovellus on rakennettu MVC-arkkitehtuurin (Model View Controller) mukaisesti. MVC-arkkitehtuurissa Model arkkitehtuurikerros sisältää sovelluksen ydintoiminnot ja rajapinnan käytettäviin tietolähteisiin, kuten esimerkiksi tietokannan tauluihin. View arkkitehtuurikerros sisältää datan näyttämiseen liittyvät toiminnollisuudet käyttöliittymässä. Controller arkkitehtuurikerros toimii datan käsittelyyn sekä näyttämiseen liittyvien kerrosten välissä, ja se sisältää sovelluksen tietovirtojen ohjaukseen liittyvät toiminnollisuudet. (Osmani 2012.)

Rakennetun sovelluksen MVC-arkkitehtuuri on esitetty kuviossa 7. Controllerina toimii app.js tiedosto joka on AngularJS arkkitehtuurin mukainen JavaScript tiedosto. Controllerin avulla ohjataan liikenne eri tiedostojen välillä käyttäjän tekemien valintojen mukaan. Käyttöliittymä on rakennettu HTML-tiedostoista, jotka sisältävät AngularJS komentoja tiedon esityskerroksessa. Käyttöliittymässä on käytetty Bootstrap tyylitiedostoa, jonka avulla voidaan rakentaa responsiivisia selainkäyttöliittymiä (Bootstrap 2014).



Kuvio 7. Uuden henkilöhakemistosovelluksen MVC-arkkitehtuuri

Sovelluksen käyttäjien autentikointi tehdään LDAP-rajapinnan kautta Active Directoryn käyttäjähakemistoon. Käyttövaltuudet sovellukseen on rakennettu roolipohjaisen

oikeusmäärittelyn mukaisesti, ja rooleja on kolmea eri tasoa. User roolissa ovat kaikki käyttäjät, joilla on käyttäjätunnus Active Directoryssä, ja he voivat muuttaa vain oman tunnuksen attribuutteja. Editor roolissa ovat ne käyttäjätunnukset, joille annetaan oikeus muokata rajatussa määrin kaikkien käyttäjien attribuutteja. Admin roolissa ovat tietohallinnon henkilöstön käyttäjätunnukset, ja he voivat käyttää kaikkia sovellukseen rakennettuja toimintoja.

Käyttäjien kirjautuessa sovellukseen, tallennetaan käyttäjätunnuksen ja oikeusroolin tiedot PHP-sessioon. Session sisältämät tiedot luetaan sovellukseen uudelleen joka kerta, kun siirrytään käyttöliittymän sivujen välillä. Oikeusroolin perusteella käyttöliittymässä näytetään vain ne toiminnot, joihin roolille on annettu valtuudet.

Lisäominaisuutena sovellukseen on rakennettu poissaolotietojen lisääminen. Käyttäjät voivat tallentaa poissaolotiedot palvelimella olevaan tietokantaan, johon tallennetaan käyttäjätunnus, alkuaika, loppuaika ja poissaolon tyyppi. Tiedot näytetään kunkin käyttäjän oman käyttäjätunnuksen attribuutteja näyttävillä sivuilla. Kaikki käyttäjät voivat muokata vain omia tietojaan. Editor ja Admin rooleissa olevat käyttäjät voivat muokata kaikkien käyttäjien poissaolotietoja.

5.3 Federoidun identiteetinhallinnan osaamisen ja teknologian kehittäminen

Opinnäytetyön toimeksiannon puitteissa pystyttiin toteuttamaan ensimmäisen vaiheen kehitystoimenpiteet kohdeorganisaation pääsyn- ja käyttövaltuushallinnan kehittämisessä. Seuraavissa vaiheissa on suosituksena federoidun identiteetinhallinnan menetelmien ja teknologian kehittäminen sekä käyttöönotto.

Seuraavien vaiheiden toteuttaminen vaatii ensin organisaation oman tietohallinnon henkilöstön osaamisen kehittämistä federoidun identiteetinhallinnan teknologian alueella. Kyseessä on kuitenkin melko monimutkainen konsepti ja siihen liittyvien käsitteiden sekä teknologioiden oppiminen vaatii aikaa. Kyseisen teknologian osaamisen kehittäminen olisi suositeltavaa ottaa tietohallinnon henkilöstön koulutusohjelmaan, jolloin avainhenkilöt kouluttautuisivat kursseilla peruskäsitteiden ja teknologioiden hallintaan.

Federoidun identiteetinhallinnan toteuttaminen on myös merkittävissä määrin neuvottelua ja sopimista. Federoitu identiteetinhallinta perustuu luottamukseen kumppaneiden välillä ja luottamuksen perusteella laaditaan sopimukset sekä luodaan tarvittavat tietotekniset edellytykset federoidun identiteetinhallinnan toteutukselle. Sovellusvuokrausta tarjoavien kumppaneiden kanssa tulisi aloittaa keskustelut siitä, miten tulevaisuudessa päästään toteuttamaan tarvittavat järjestelyt tekniselle toteutukselle.

Organisaatiossa on jo nykyisessä toimintaympäristössä käytetty Microsoftin DirSync työkalua, jolla saadaan siirrettyä Active Directory hakemistopalvelusta käyttäjätunnukset ja salasanat Office 365-pilvipalveluun. DirSync siirtää tunnukset ja salasanat, mutta käyttäjien pitää silti kirjautua erikseen sisään Office 365-palveluun. Mikäli halutaan kirjautumisen tapahtuvan automaattisesti ilman salasanan syöttämistä kertakirjautumisen tapaan, tulee organisaation laajentaa arkkitehtuuria Active Directory Federation Services (AD FS) palveluilla. (Andrew 2014.)

Teknologisten valmiuksien kehittämisen näkökulmasta kohdeorganisaation on suositeltavaa rakentaa oma Identity Provider (IdP) tunnistuspalvelu. Koska organisaatio käyttää Microsoftin teknologiaa, on suositeltavana teknisenä vaihtoehtona Microsoft Active Directory Federation Services (AD FS) arkkitehtuurin rakentaminen organisaation käyttöön. Oman tunnistuspalvelun käyttöä voi laajentaa tulevaisuudessa Office 365-palvelun lisäksi yhteistyökumppaneiden sovelluksiin, jolloin saataisiin SaaS-sovellukset saman käyttäjätunnistuksen ja salasanan piiriin. Ratkaisu mahdollistaisi myös muiden pilvipalveluihin rakennettavien sovellusten autentikoinnin kotiorganisaation tunnistuspalvelun kautta.

6 Yhteenveto

Aihealue on ollut mielestäni haasteellinen ja vaativa, ehkä jopa vaikein aihealue tietotekniikassa. Käytännön työelämässä olen usein kohdannut autentikoinnin ja käyttövaltuushallinnan järjestämisen ongelmia ulkopuolisten tietojärjestelmien toimittajien kanssa. Tietojärjestelmiä hankittaessa on niiden autentikoinnin liittäminen omaan käyttäjähakemistoon yleensä aina tavoitteena. SaaS-sovellusvuokrauksen ja pilvipalvelujen yleistyessä tekniset ongelmat ovat kuitenkin olleet merkittäviä ja liitosta ei ole pystytty toteuttamaan.

Opinnäytetyön teoriaosuuden selvittämisen aikana aihealueen laajuus oli yllättävää. Teknologioita ja kehitettyjä menetelmiä on laaja kirjo ja usein oli vaikeata löytää oman työn kannalta oleelliset tiedot. Toisaalta täytyi tehdä paljon rajausta sen suhteen mitä otetaan mukaan työhön. Muuten informaation laajuus olisi haitannut keskittymistä toimeksiantajan näkökulmasta tarpeellisten asioiden selvittämiseen. Hyvän kuvan identiteetin hallinnan laajuudesta saa aihepiiriin liittyvistä standardoinnin hankkeista. Merkittäviä kehitettyjä standardeja ovat information card, SAML ja OpenID. Kehittymässä on myös muita standardeja, kuten OAuth ja OpenSocial. (Bertino & Takahashi 2011, 76–78.)

Merkittävää oli huomata se, että vaikka teknologia on merkittävä osa tietoteknisissä hankkeissa, niin ihmisten toiminta ja noudatettavat prosessit ovat vähintään yhtä tärkeä osa kokonaisuutta. Tekniset ratkaisut eivät useinkaan riitä, vaan toiminnan organisoiminen tiedon käsittelyn toteuttamiseksi on välttämätöntä. Suuri työmäärä liittyy myös nykytilanteen selvittämiseen, joka on kuitenkin peruslähtökohta kehitystoimenpiteiden suunnittelulle.

Työntekijän roolissa ihmisten toiminta rajautuu helposti vain oman työtehtävän vaatimalle alueelle. Tällöin kokonaiskuva usein hämärtyy ja tehdään vain välttämättömät toimenpiteet ja kehittämishankkeet omalla vastuualueella olevien asioiden hoitamiseksi. Toisaalta kokonaisuuden hallinnan vastuu jää epämääräiseksi, kun erillisiä ongelmia ratkotaan asia kerrallaan ja ei haluta tarttua vaikeammin ratkaistaviin koko organisaation toiminta- ja tietoarkkitehtuuriin liittyviin ongelmiin.

Uuden henkilöhakemistosovelluksen rakentaminen oli mielenkiintoista ja opettavaista. Sovelluksen rakentaminen oli pienimuotoinen ohjelmistokehitysprojekti, jossa toiminnalliset vaatimukset olivat ennalta määrättyjä aiemmin käytössä olleen ratkaisun pohjalta. Haasteita tuottivat kuitenkin lukuisat tekniset yksityiskohdat, joiden ratkaisemiseen saattoi kulua huomattavan paljon aikaa. AngularJS arkkitehtuuri käyttöliittymän rakentamisessa osoittautui hyvin toimivaksi ja sen avulla pystyttiin kehittämään perustoiminnollisuudet nopeassa aikataulussa. Palvelimella toimivat rajapinnat tietolähteisiin on rakennettu Linux palvelimelle PHP-kielellä, mutta yhtä hyvin ne voitaisiin rakentaa Microsoftin C#-kielellä, jolloin voitaisiin käyttää Microsoft Windows palvelimia.

Varsinainen opinnäytetyöprosessi toteutui suunnitelman mukaisesti, mutta työmäärä osoittautui arvioitua suuremmaksi. Tämä johtui siitä, että työhön otettiin mukaan myös henkilöhakemistosovelluksen rakentaminen, koska sovelluksen merkitys toimeksiantajan organisaatiossa oli niin merkittävä. Opinnäytetyön kirjoittaminen vaati kurinalaista keskittymistä kirjoittamiseen ja lähdemateriaalin etsimiseen sekä lähteiden hyödyntämiseen teoriaosuuden rakentamisessa.

Lähteet

Andrew, P. 2014. Synchronizing your directory with Office 365 is easy. Office Blogs. Microsoft. Luettavissa: http://blogs.office.com/2014/04/15/synchronizing-your-directory-with-office-365-is-easy/. Luettu: 5.10.2014.

AngularJS. 2014. AngularJS by Google. HTML enhanced for web apps! Google. Luettavissa: https://angularjs.org/. Luettu: 27.9.2014.

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030.

Bertino, E. & Takahashi, K. 2011. Identity Management, Concepts, Technologies, and Systems. ARTECH HOUSE. Boston. London.

Bootstrap. 2014. Bootstrap is the most popular HTML, CSS, and JS framework for developing responsive, mobile first projects on the web. Luettavissa: http://getbootstrap.com/. Luettu: 26.10.2014.

Boyle, R. & Panko, R. 2014. Pearson New International Edition. Corporate Computer Security. Third Edition. Pearson Education Limited 2014. United States of America.

CSC. 2014. Haka-käyttäjätunnistusjärjestelmä ja -luottamusverkosto. CSC - Tieteen tietotekniikan keskus Oy. Luettavissa: https://confluence.csc.fi/pages/viewpage.action?pageId=29395721. Luettu: 27.9.2014.

Henkilötietolaki 22.4.1999/523.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617.

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.

Linden, M. 2009. Organisational and cross-organisational identity management. Tampereen yliopistopaino. Tampere. Luettavissa: http://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/149/linden.pdf. Luettu: 14.9.2014.

Linden, M. 9.1.2012. Identiteetin- ja pääsynhallinta. Luentomoniste. Tampereen teknillinen yliopisto. Tampere. Luettavissa. http://www.cs.tut.fi/~linden/iam-pruju.pdf. Luettu: 13.9.2014.

Linden, M (toim.). & Kurtti, N. & Palvalin, M. & Numminen, M. & Rajala, H. & Holmberg, J. & Mäkelä, J. & Järvenpää, T. & Kuusinen, J. & Tuomela, M. & Vuorinen, A. 2011. Identiteetin- ja pääsynhallinta. Seminaariraportti. Tampereen teknillinen yliopisto. Tampere. Luettavissa: http://www.cs.tut.fi/kurssit/TLT-3600/iam-sem2011.pdf. Luettu: 13.9.2014.

Osmani, A. 2012. Journey Through The JavaScript MVC Jungle. SMASHING MAGAZINE. Luettavissa: http://www.smashingmagazine.com/2012/07/27/journey-through-the-javascript-mvc-jungle/. Luettu: 26.10.2014.

Seitsonen, M. & Haukilehto, A. 6.3.2013. Senior-konsultit Soveltosta. Federointi kertakirjautumisen mahdollistajana. Microsoft TechDays 2013. Seminaariesitys. Helsinki. Luettavissa: https://www.youtube.com/watch?v=Mt3OpcqJkw8. Luettu: 5.10.2014.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681.

Valtori. 2014. Kertakirjautumisratkaisu Virtu. Valtion tieto- ja viestintätekniikkakeskus, käyttöpalvelut. Luettavissa: http://www.valtori.fi/fi-FI/Palvelut/Kayttopalvelut. Luettu: 27.9.2014.

VAHTI 9/2006. 2006. Käyttövaltuushallinnon hyvät periaatteet ja käytännöt. Valtiovarainministeriö. Helsinki. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061122Kaeytt oe/vahti_9_06.pdf Luettu: 20.9.2014.